MUP.PK.III.SG.371 – 65/11 Lublin, dnia 07.07.2011 r.

Działając na podstawie art. 38 ust 4 ustawy z dnia 29. 01. 2004 r. prawo zamówień publicznych (tj. Dz. U. z 2010 Nr 113, poz. 759 z późn.) zwanej dalej ustawą, Zamawiający w ramach prowadzonego postępowania w celu udzielenia zamówienia na dostawę sprzętu i oprogramowania informatycznego oraz materiałów eksploatacyjnych, dokonuje **zmiany treści Specyfikacji Istotnych Warunków Zamówienia** poprzez :

MODYFIKACJĘ SPECYFIKACJI ISTOTNYCH WARUNKÓW ZAMÓWIENIA W ZAKRESIE PUNKTU 4 – „**Opis szczegółowy części przedmiotu zamówienia"** w zakresie części II postępowania: **Dostawa redundantnego klastra HA dwóch urządzeń UTM**

W SPOSÓB NASTĘPUJĄCY:

Brzmienie aktualne opisu przedmiotu zamówienia Część II (po modyfikacji)

CZĘŚĆ II
Dostawa redundantnego klastra HA dwóch urządzeń UTM

Minimalne *Parametry systemu:*

- Obudowa musi umożliwiać montaż urządzenia w szafie rack 19" (muszą być dołączono wszystkie elementy konieczne do montażu)
- System ochrony musi być zbudowany przy użyciu minimalnej ilości elementów ruchomych, krytycznych dla jego działania, dlatego główne urządzenie ochronne nie może posiadać twardego dysku lecz musi w zamian używać pamięci FLASH.
- Podstawowe funkcje systemu muszą być realizowane sprzętowo, przy użyciu wyspecjalizowanych układów ASIC
- Dla zapewnienia wysokiej sprawności i skuteczności działania systemu urządzenia ochronne musza pracować w oparciu o dedykowany system operacyjny; nie dopuszcza się stosowania systemów operacyjnych ogólnego przeznaczenia
- Wszystkie funkcje ochronne oraz zastosowane technologie, w tym system operacyjny musi pochodzić od jednego producenta, który udzieli odbiorcy licencji bez limitu chronionych użytkowników (licencja na urządzenie).
- Dla systemu urządzenia musi być dostępna zewnętrzna sprzętowa platforma centralnego zarządzania pochodząca od tego samego producenta.
- System musi umożliwiać aktualizację oprogramowania oraz zapisywanie i odtwarzanie konfiguracji z pamięci USB
- Wymagana jest funkcja monitoringu i wykrywania uszkodzeń elementów sprzętowych i programowych systemu zabezpieczeń i łączy sieciowych.
- System musi mieć możliwość współpracy z zewnętrznym, sprzętowym modułem raportowania i korelacji logów umożliwiającym:
  - zbieranie logów z urządzeń bezpieczeństwa
  - generowanie raportów
  - skanowanie podatności stacji w sieci
  - zdalną kwarantannę dla modułu antywirusowego
- Musi być zapewniona możliwość połączenia 2 identycznych urządzeń w klaster typu Active-Active lub Active-Passive
- **System musi posiadać nie mniej niż 16 interfejsów sieciowych Ethernet, w tym nie mniej niż 8 interfejsów Ethernet 10/100/1000 Base-TX**

* Wymagana funkcjonalność:
  Podstawowa:
  - kontrola dostępu - zapora ogniowa klasy Stateful Inspection
  - ochronę przed wirusami – antywirus [AV] (dla protokołów SMTP, POP3, IMAP, HTTP, FTP, IM, NNTP)
  - poufność danych - IPSec VPN oraz SSL VPN
  - ochronę przed atakami - Intrusion Prevention System [IPS/IDS]

  Dodatkowa:
  - kontrolę treści i kategoryzację odwiedzanych stron WWW – Web\URL Filter
  - kontrolę zawartości poczty – antyspam [AS] (dla protokołów SMTP, POP3, IMAP)
  - kontrolę pasma oraz ruchu [QoS, Traffic shaping]
  - kontrolę aplikacji (wsparcie dla co najmniej tysiąca aplikacji w tym IM, P2P, VoIP, Web-mail)
  - zapobieganie przed wyciekiem informacji poufnej - DLP (Data Leak Prevention)
  - SSL proxy z możliwością pełniej analizy szyfrowanej komunikacji dla wybranych protokołów (HTTPS, IMAPS, POP3S, SMTPS)
  - funkcjonalność kontrolera sieci bezprzewodowej (we współpracy z punktami dostępowymi tego samego producenta)
* Urządzenie musi zapewniać
  - obsługę nie mniej niż 500.000 jednoczesnych połączeń i 15.000 nowych połączeń na sekundę
  - przepływność nie mniejszą niż 5 Gbs dla ruchu nieszyfrowanego i 2,5 Gbs dla VPN (3DES)
  - obsługę nie mniej niż 2.000 jednoczesnych tuneli VPN
  - możliwość konfiguracji przez terminal i linię komend oraz konsolę graficzną (GUI).
  - zabezpieczony poprzez szyfrowanie dostęp do urządzenia i zarządzanie nim z sieci
  - możliwość definiowania wielu administratorów o różnych uprawnieniach, którzy będą uwierzytelniani za pomocą haseł statycznych i haseł dynamicznych (RADIUS, RSA SecureID)

Zasady działania:

* Urządzenie musi dawać możliwość ustawienia następujących trybów pracy:
  - jako router/NAT (3.warstwa ISO-OSI) lub
  - jako most (transparent bridge). Tryb przezroczysty musi umożliwiać wdrożenie urządzenia bez modyfikacji topologii sieci niemal w dowolnym jej miejscu lub
  - Jako router i most jednocześnie (tryb hybrydowy)
* Urządzenie musi umożliwiać utworzenie nie mniej niż 6000 polityk bezpieczeństwa firewall'a, przy czym każda musi uwzględniać adresy IP, interfejsy, protokoły i usługi sieciowe, użytkowników aplikacji, domeny, reakcje zabezpieczeń, rejestrowanie zdarzeń i alarmowanie, zarządzanie pasmem sieci (m.in. pasma gwarantowane i maksymalne, priorytety, oznaczenia DiffServ).
* Urządzenie musi zapewniać wykrywanie i blokowanie technik oraz ataków stosowanych przez hakerów (m.in. IP Spoofing, SYN Attack, ICMP Flood, UDP Flood, Port Scan) i niebezpiecznych komponentów (m.in. Java/ActiveX) – nie mniej niż 4000 sygnatur ataków
* Aktualizacja bazy sygnatur musi odbywać się ręcznie lub automatycznie,
* Musi zapewniać możliwość dodawania własnych sygnatur ataków,
* Urządzenie musi chronić sieć VPN przed atakami Replay Attack oraz limitować maksymalną liczbę otwartych sesji z jednego adresu IP

* Możliwość wykrywania anomalii protokołów i ruchu
* Ochrona antywirusowa musi mieć możliwość transferu częściowo przeskanowanego pliku do klienta by uniknąć przekroczenia dopuszczalnego czasu oczekiwania (timeout).
* Antywirus powinien przeprowadzać sprawdzanie danych zarówno po bazie sygnatur wirusów jak i heurystycznie
* Mechanizm antyspamowy powinien pracować w obrębie protokołów SMTP, POP3, IMAP, SMTPS, POP3S i IMAPS.
* Klasyfikacja wiadomości powinna bazować na wielu czynnikach, takich jak:
  - sprawdzenie zdefiniowanych przez administratora adresów IP hostów, które brały udział w dostarczeniu wiadomości,
  - sprawdzenie zdefiniowanych przez administratora adresów pocztowych,
  - ogólnodostępnych baz RBL, ORDBL
  - sprawdzenie treści pod kątem zadanych przez administratora słów kluczowych
  - musi też umożliwiać korzystanie z zewnętrznej, wieloczynnikowej bazy spamu.
* Filtracja stron www musi umożliwiać blokowanie stron w oparciu o :
  - białe i czarne listy URL
  - o zawarte w stronie słowa kluczowe
  - dynamicznie definiowane kategorie.
* Urządzenie musi obsługiwać
  - statyczną i dynamiczną translację adresów (NAT)
  - Translację NAPT
  - NAT traversal dla protokołów SIP i H323
* Musi istnieć możliwość definiowania w jednym urządzeniu, bez dodatkowych licencji, nie mniej niż 10 wirtualnych firewalli, gdzie każdy z nich posiada indywidualne tabele routingu, polityki bezpieczeństwa i dostęp administracyjny.
* Musi być zapewniona obsługa Policy Routingu w oparciu o typ protokołu, numer portu, interfejsu, adresu IP źródłowego oraz docelowego.
* Protokoły routingu dynamicznego, nie mniej niż RIPv2, OSPF, BGP-4 i PIM.
* Dostawca musi udostępniać klienta VPN własnej produkcji realizującego następujące mechanizmy ochrony końcówki:
  - firewall
  - antywirus
  - web filtering
  - antyspam
* Konfiguracja połączeń VPN w oparciu o politykę bezpieczeństwa i tabele routingu
* Muszą być zapewnione następujące funkcje VPN:
  - Monitorowanie stanu tuneli VPN i stałego utrzymywania ich aktywności
  - Tworzenie połączeń w topologii Site-to-Site oraz Client-to-Site
  - Obsługa mechanizmów: IPSec NAT Traversal, DPD, XAuth
* Musi być umożliwione wykonywanie uwierzytelniania tożsamości użytkowników za pomocą nie mniej niż:
  - haseł statycznych i definicji użytkowników przechowywanych w lokalnej bazie urządzenia,
  - haseł statycznych i definicji użytkowników przechowywanych w bazach zgodnych z LDAP
  - haseł dynamicznych (RADIUS, RSA SecureID) w oparciu o zewnętrzne bazy danych
* Musi być też zapewniona możliwość, bez żadnych dodatkowych opłat licencyjnych, budowania logowania Single Sign On w środowisku Active Directory.

Licencje i serwis:

* Wykonawca musi dostarczyć licencje aktywacyjne dla funkcji bezpieczeństwa na okres 12 miesięcy. Licencja aktywna od instalacji i konfiguracji sprzętu w siedzibie Zamawiającego.
* Serwis gwarancyjny producenta na system: 12 miesięcy
* Zamawiający wymaga aby oferowany sprzęt objęty był serwisem gwarancyjnym u dystrybutora na terenie Polski
* Wykonawca musi najpóźniej do dnia podpisania umowy okazać zaświadczenie o możliwości przyjęcia uszkodzonego urządzenia objętego serwisem gwarancyjnym do naprawy u dystrybutora na terenie Polski.

* Wykonawca musi dysponować co najmniej dwoma osobami posiadającymi tytuł „inżyniera" nadany przez producenta sprzętu, posiadającymi aktualne certyfikaty techniczne producenta do instalacji i konfiguracji sprzętu

Zaoferowany towar musi być fabrycznie nowy i fabrycznie zapakowany.

Zmiana treści SIWZ dokonana przez Zamawiającego została zaznaczona poprzez pogrubienie czcionki oraz podkreślenie.

W związku z dokonaną modyfikacją Zamawiający informuje, iż nie ulega zmianie termin składania i otwarcia ofert.

Z poważaniem

Z up. Prezydenta Miasta Lublin
Zastępca Dyrektora
Miejskiego Urzędu Pracy w Lublinie
mgr Monika Rynkar